AUDIT REPORT

~~OFFICIAL USE ONLY~~
~~SECURITY RELATED INFORMATION~~

Office of the Inspector General Computer Security Audit of the Technical Training Center – Chattanooga, Tennessee

OIG-06-A-19 July 11, 2006

Nuclear Regulatory Commission
Fiscal Year 2006 Computer Security Audit
Report of Findings

Office of the Inspector General Computer Security Audit of the Technical Training Center – Chattanooga, TN

TABLE OF CONTENTS

Nuclear Regulatory Commission
Fiscal Year 2006 Computer Security Audit

EXECUTIVE SUMMARY

Background

The U.S. Nuclear Regulatory Commission (NRC) has in place the Technical Training Center (TTC) to provide training for the NRC headquarters and regional staff in various technical disciplines associated with the regulation of nuclear materials and facilities. The TTC is part of the Office of Human Resources (HR) and operates under the direction of the Associate Director for Training and Development.

Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorizations of Federal Information and Information Systems*, defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NRC depends heavily on information systems security measures to avoid data tampering, fraud, inappropriate access, disclosure of sensitive information, and disruptions in critical operations. It is NRC's policy to maintain an automated information systems security program to provide appropriate administrative, technical, and physical security measures for the protection of the information resources. Security measures at the Regions and the TTC were last assessed in 2003.

The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, requires agencies to implement and maintain an automated information systems security program, including the preparation of policies, standards and procedures. In addition, the Federal Information Security Management Act (FISMA) of 2002 outlines the information security management requirements for agencies. These requirements include an independent evaluation of an agency's information security program and practices, and an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards and guidelines.

Purpose/Objectives

The objectives of the computer security audit of the NRC TTC office were to:

1. Evaluate the adequacy of the information security program and practices;
2. Evaluate the effectiveness of the information security control techniques; and
3. Evaluate the progress towards resolving information security program weaknesses identified during the FY 2003 Computer Security Audit.

Results in Brief

The TTC's information security program and practices are not always consistent with the NRC's Automated Information Systems (AIS) security program as defined in Management Directive (MD) 12.5, *NRC Automated Information Systems Security Program,* and FISMA, OMB and National Institute of Standards and Technology (NIST) guidance. While many of the TTC automated and manual security controls are generally effective, some security controls need improvement.

Physical Access Controls

The TTC is implementing most of the physical access controls outlined in MD 12.5. These controls include adequate physical access controls to the TTC facility. However, there is an excessive number of personnel with access to the computer rooms and combinations are not changed on a periodic basis for keypads located at the TTC facility. In addition, key inventories are not performed on a semiannual basis.

Logical Access Controls

The TTC is implementing most of the logical access controls outlined in MD 12.5. These controls include appropriate user account management for system access for all employees. However, users have the ability to change or disable screen saver locks on their local workstations. Additionally, policies and procedures have not been implemented at the TTC regarding the tracking of equipment and media that has been sanitized or disposed.

Recommendations

A consolidated list of recommendations made to the Executive Director for Operations is on page 9.

I. Background

NRC has in place the TTC to provide training for the NRC headquarters and regional staff in various technical disciplines associated with the regulation of nuclear materials and facilities. The TTC is part of HR and operates under the direction of the Associate Director for Training and Development.

FIPS 199, *Standards for Security Categorizations of Federal Information and Information Systems*, defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NRC depends heavily on information systems security measures to avoid data tampering, fraud, inappropriate access and disclosure of sensitive information, and disruptions in critical operations. It is NRC's policy to maintain an automated information systems security program to provide appropriate administrative, technical, and physical security measures for the protection of the information resources. Security measures at the Regions and the TTC were last assessed in 2003.

OMB Circular A-130, *Management of Federal Information Resource*, Appendix III, requires agencies to implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures.

FISMA was enacted into law as Title III of the E-Government Act of 2002 (P.L. 107-347, December 17, 2002). Key FISMA requirements include:

- The establishment of agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques, training requirements, periodic testing and evaluation, reporting, plans for remedial action, security incident response, and continuity of operations.

- An annual independent evaluation of the federal agency's information security programs and practices.

- An assessment of compliance with the requirements of the Act.

General computer controls are the structure, policies, and procedures that apply to an entity's overall computer operations and help ensure their proper operation. The following general computer controls are primary objectives of an effective computer security program:

Physical Access

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment.

Logical Access

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers, passwords, or other identifiers that are linked to predetermined access privileges.

Security Program and Planning

The Security Program provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

Continuity of Operations and Recovery

Continuity of operations and recovery controls ensure that, when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected.

Configuration Management

Configuration management controls prevent unauthorized programs or modifications to an existing program from being implemented.

II. Audit Criteria (Laws, Regulations, and Guidance)

The TTC security audit was performed in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's Government Auditing Standards, 2003 revision, and the Federal Information System Controls Audit Manual (FISCAM) (June 2001 version). The methodology included verifying compliance with the OMB Circulars' guidance that applied to our computer security audit.

Specifically, the audit methodology was guided by additional NRC and Federal criteria, which include, but are not limited to:

- Information Systems Audit and Control Association Audit Standards;
- OMB Circulars (A-130, A-123 and A-127);
- NIST Special Publications (SP) related to computer-based information security (i.e. 800-12, 800-18, 800-26, 800-53).

III. Findings and Recommendations

The TTC has made significant improvements within its information technology (IT) general controls environment since the security audit completed in 2003 by implementing corrective actions to previously identified conditions. However, the TTC's information security program and practices are not always consistent with the NRC's automated information systems security program as defined in MD 12.5 and Federal criteria generated by OMB and NIST. While many of the TTC's automated and manual security controls are generally effective, some security controls need improvement. Specifics on these matters are described in the following sections.

A. Physical Access Controls

1. Excessive number of personnel with access to the computer rooms.

An excessive number of personnel have access to the computer rooms at the TTC facility. TTC personnel noted that managers have access to the TTC computer rooms to serve as backups. If access is not limited to personnel with a legitimate need for that access, the risk of resources being compromised becomes greater.

MD 12.5, Appendix A, Section 4.2 states: "Limit access to the computer and AIS equipment rooms in which network equipment resides to those personnel who must access the rooms to perform their duties, such as network and system administrators and telecommunication technicians."

Recommendation

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Limit the number of individuals with access to the sensitive/restricted areas of the TTC facility such as the computer rooms.

2. Records of key inventories are not kept.

The TTC is conducting key inventories on a semiannual basis; however, records have not been kept supporting the inventories. Therefore, we were unable to verify that the inventories were being done a semiannual basis. If key inventories are not conducted on a semiannual basis then tracking keys

and identifying lost keys becomes more difficult. MD 12.5 Appendix A, Section 4.3 states: "Semiannual inventories of all keys should be conducted and recorded. Maintain the inventories as official records for 1 year after they are no longer current."

Recommendation

The Office of the Inspector General recommends that the Executive Director for Operations:

2. Conduct inventories of all keys on a semiannual basis and maintain records on the inventories.

3. Keypad combinations are not changed on a periodic basis.

Combinations are not changed on a periodic basis for keypads located at the TTC facility because they are not used at main entry points to the NRC occupied areas. Key codes should be periodically changed to prevent reentry by previous visitors who might have become knowledgeable of the code. Physical security controls not being implemented will not serve their intended purpose to restrict physical access to computer resources and protect them from intentional loss and/or impairment.

MD 12.5, Appendix A, Section 4.3 states: "It is essential for the protection of all NRC AIS assets that the sponsoring office establish, document, implement, and enforce effective key and combination control procedures. When individuals no longer have a need for access, ensure that combinations are changed immediately."

Recommendation

The Office of the Inspector General recommends that the Executive Director for Operations:

3. Change the combinations of the keypads on a periodic basis or remove/disable the keypads.

B. Logical Access Controls

4. Users have the ability to disable the screen saver password lock from recommended settings on their local computers.

Local users at the TTC are able to change the default screen saver settings on their local workstation or disable the screen-saver lock. This occurs because the Group Policy that is controlled from Headquarters is not set up correctly or it has been modified. MD 12.5, Part 2, Section 2.5, requires that the screen-saver password protection is enabled to ensure that the screen-saver turns on after fifteen minutes of inactivity. Therefore, if an employee leaves their workstation unattended for fifteen or more minutes the screen saver will enable and can only be turned off when the user enters their password. If a user disables the screen saver password lock then the user will remain logged into the system. Without automatic session termination after a specified period of inactivity, the risk of loss, alteration and/or unauthorized disclosure of NRC information, increases.

Recommendation

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Verify group policy settings at Headquarters and test workstations at the TTC to ensure that the screen saver lock policy is working properly.

5. No tracking of sanitized equipment and media.

The TTC uses the locally developed Property Management System for the tracking of NRC owned property, including hardware and software. However, the system does not track when and by whom the equipment has been wiped because policies and procedure have not been implemented by the TTC. For example, the TTC recently had a refresh and disposed of sixty nine machines however the information was not properly documented. Without maintaining an audit trail of the IT equipment and media that has been sanitized, the determination of how, when, and by whom specific actions were taken may be difficult if not impossible.

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook Section 14.6 Documentation* states: "Documentation of all aspects of computer support and operations is important to ensure continuity and

consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently."

Recommendation

The Office of the Inspector General recommends that the Executive Director for Operations:

5. Develop and implement policies and procedures regarding the tracking of equipment and media that have been sanitized or disposed and record the information in the Property Management System.

IV. Consolidated List of Recommendations

OIG recommends that the Executive Director for Operations:

1. Limit the number of individuals with access to the sensitive/restricted areas of the TTC facility such as the computer rooms.

2. Conduct inventories of all keys on a semiannual basis and maintain records on the inventories.

3. Change the combinations of the keypads on a periodic basis or remove/disable the keypads.

4. Verify group policy settings at Headquarters and test workstations at the TTC to ensure that the screen saver lock policy is working properly.

5. Develop and implement policies and procedures regarding the tracking of equipment and media that have been sanitized or disposed and record the information in the Property Management System.

Appendix A: Scope and Methodology

The objectives of the computer security audit of the TTC office were to:

1. Evaluate the adequacy of the information security program and practices;
2. Evaluate the effectiveness of the information security control techniques; and
3. Evaluate the progress towards resolving information security program weaknesses identified during FY 2003 Computer Security Audit.

The scope of this computer security audit included:

- The four floors that the TTC office occupies in the Osborne Office Center, 5746 Marlin Road, Chattanooga, TN 37411
- The TTC Local Area Network (LAN) equipment
- IT equipment that supports the simulators
- Other internal TTC applications

The computer security audit did not include controls related to the management of safeguards or classified information.

In conducting our audit of the TTC's computer security program and practices, the following areas were reviewed: physical and logical access controls, security program and planning, continuity of operation planning and configuration management controls. Specifically, the security audit team conducted a site survey of the four floors that the TTC occupies at the Osborne Office Center, focusing on the areas that house IT equipment. The team conducted interviews with the LAN system administrator and the TTC Information System Security Officer (ISSO). The security audit team also conducted interviews with other TTC staff members. The team reviewed documentation provided by TTC including floor plans, network diagrams, organizational charts, key control procedures, contingency plans, documented backup procedures, and the Occupant Emergency Plan.

This work was conducted during a site visit to the TTC office between April 3 and 6, 2006. The work was conducted by Scott Riggenbach, Sarah Mirzakhani and Kerri Posteraro from Urbach Kahn and Werlin LLP.

Appendix B: Acronym List

Acronym	Description
AIS	Automated Information System
FISCAM	Federal Information System Controls Audit Manual
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
LAN	Local Area Network
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OMB	Office of Management and Budget
SP	Special Publication
TTC	Technical Training Center